**Содержание**

Введение

1. Информационная безопасность государства
2. Влияние защищенности российского сегмента глобальной сети Интернет на состояние информационной безопасности государства

Заключение

Литература

**Введение**

Проблемы обеспечения информационной безопасности России в той или иной степени находят свое отражение не только в исследованиях и теоретических разработках отечественных и зарубежных ученых, но и в официальных документах. Такие понятия, как: «национальная безопасность», «информационная безопасность», «информационная организация государства» закладываются в основание различного рода политических доктрин и концепций большинства общественных, политических организаций и движений страны. Они стали предметом законотворческого процесса, привлекают пристальное внимание средств массовой информации.

Наряду с тем, что в большинстве сфер деятельности государства происходят позитивные изменения в реализации реформ, необходимо подчеркнуть, что развитие информационной организации государства объективно переживает сложный период. В результате информационная сфера, ее ресурсы, в том числе и их защищенность, отстают в развитии от других институтов современного российского общества. Данное обстоятельство негативно сказывается не только на информационной организации государства, но и на состоянии информационной безопасности России, информационной безопасности личности и всего общества в целом.

Важнейшую роль в обеспечении информационной безопасности государства, несомненно, играет его защищенность, создаваемая государством посредством ряда мероприятий и призванная противостоять реальным и потенциальным угрозам национальной безопасности, исходящим как извне, так и возникающим внутри страны.

**1 Информационная безопасность государства**

Проблемы обеспечения информационной безопасности федеральными органами законодательной и исполнительной власти Российской Федерации, политическим руководством страны, учеными и практиками воспринимаются как одни из наиболее актуальных и жизненно важных для современного состояния и перспектив развития российской государственности, демократии, гарантий защиты интересов общества и личности. Социально-политическая рефлексия данных проблем в значительной степени определяется динамикой современных политических процессов, связанных с формированием нового миропорядка, объективными процессами изменения роли и места России на мировой политической арене, происходящими на фоне кризисных явлений в ходе модернизации Российского государства, в том числе и в информационной сфере.

Вопросы обеспечения информационной безопасности, непосредственно связанные с реформированием информационной организации государства, находят свое приоритетное отражение в политических заявлениях государственных и общественных деятелей различного уровня, в концептуальных установках общественных движений и политических организаций и их лидеров.

Понятие «безопасность» современными учеными и практиками рассматривается с самых различных позиций. Однако наиболее распространенным стал подход, согласно которому под безопасностью понимается «состояние защищенности общества и его составляющих от внутренних и внешних угроз, являющееся свойством социальной системы». Такой подход закреплен и в Законе Российской Федерации «О безопасности», в статье 1, которого безопасность определена как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

Понятие «безопасность» непосредственно связано с другими определениями, - такими, как: «интересы», «угроза», «опасность», «защита» и т.д.

Некоторые эксперты представляют безопасность как систему гарантий защиты жизненно важных интересов государства, общества и личности внутри и вне страны. Она может проявляться на различных уровнях: мирового сообщества, региона, отдельного государства, социальной общности и личности. Говоря о безопасности того или иного объекта, имеется в виду защищенность жизненно важных интересов данного объекта от внешних и внутренних угроз. Следуя этой логике, он дает следующее определение понятия «информационная безопасность»: «...информационная безопасность – это защищенность жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз.

Информационная сфера становится не только важнейшей сферой международного сотрудничества, но и объектом соперничества. Проблемы в сфере информационных отношений, формирования информационных ресурсов и пользования ими обостряются вследствие политического и экономического противоборства различных государств, имеющего место информационного неравенства.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность - сложное системное, многоуровневое явление, на состояние и перспективы развития которого оказывают непосредственное воздействие внешние и внутренние факторы. Наиболее важными из них являются:

* политическая обстановка в мире;
* наличие потенциальных внешних и внутренних угроз;
* состояние и уровень информационно-коммуникационного развития страны;
* внутриполитическая обстановка в государстве.

Важной стороной информационной безопасности государства является достижение состояния его защищенности, то есть, – создание и поддержание инженерно-технической мощи и информационной организации, соответствующими реальным и потенциальным угрозам, а также демографическому и экономическому состоянию страны.

В Концепции национальной безопасности Российской Федерации подчеркивается факт усиления угроз национальной безопасности Российской Федерации в информационной сфере: «Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним».

**2 Влияние защищенности российского сегмента глобальной сети Интернет на состояние информационной безопасности государства**

Многоплановость и неоднозначность воздействия различных факторов на взаимодействие защиты информационного пространства и информационной безопасности позволяет выделить группы факторов объективного и субъективного характера.

Объективные факторы являют собой многоуровневую систему (глобального, регионального и национально-государственного уровней) внутренних и внешних параметров, воздействующих на субъекты формирования и реализации информационной политики государства.

К числу наиболее значимых объективных факторов в современных условиях, обусловливающих влияние защиты информационного пространства на информационную безопасность, относятся геополитические факторы – геополитические параметры (условия, ресурсы, возможности), определяющие состояние и развитие государств, регионов и мира в целом.

Геополитические параметры государства являются определяющими в дихотомии «защита информационного пространства – информационная безопасность», поскольку именно они определяют в условиях формирования нового мирового порядка специфику и возможности государства осуществлять защиту информационного пространства и, соответственно, обеспечивать свою информационную безопасность.

Любое государство, приступая к формированию своей информационной политики или внося в нее коррективы, должно учитывать воздействие геополитических факторов и тех угроз, которые они провоцируют.

К объективным факторам с полным основанием можно отнести также климатические условия, демографическую ситуацию в стране и целый ряд других параметров, объективно определяющих место государства в мировом сообществе. Поэтому анализ «отличительных начал» государства и соответствия им информационной системы государства является важным условием влияния защиты информационного пространства на информационную безопасность.

Наряду с объективными факторами исследуемого процесса на него оказывают воздействие также факторы субъективного свойства, представляющие собой результаты многоплановой деятельности субъектов информационной политики (защиты информационного пространства) конкретного государства (группы государств) в области его (их) информационной безопасности.

В данном случае речь идет, прежде всего, о политической деятельности и практических действиях конкретных государств, политических сил и различных организаций (в том числе и экстремистских, террористических), негативно воздействующих на политическую обстановку в мире, стране, определяя состояние опасностей и угроз информационной безопасности конкретного государства. Помимо этого к факторам субъективного порядка относится также деятельность субъектов информационной политики данного государства (органов государственной власти, структур информационной организации и систем, обеспечивающих ее жизнедеятельность и развитие), осуществляющего защиту информационного пространства и реализующего задачи обеспечения информационной безопасности. Влияние субъективных факторов в данном случае предполагает результат осознанной деятельности субъектов политики в процессе их воздействия на информационную безопасность государства, опосредованную спецификой, содержанием и результатами защиты информационного пространства.

Исходя из того, что информационная безопасность на рубеже третьего тысячелетия выходит на первое место в системе национальной безопасности, формирование и проведение единой государственной политики в этой сфере приобретает приоритетное значение.

Поскольку всякая политика в правовом государстве должна строиться на основе права, крайне важно определить, какие правовые основы необходимо создать. Пока можно констатировать, что развитие общественных отношений в этой сфере существенно опережает развитие права по этим вопросам.

Сегодня сложились две тенденции в органах государственной власти в определении понятия и структуры информационной безопасности. Представители гуманитарного направления связывают информационную безопасность только с институтом тайны. Представители так называемых «силовых структур» предлагают распространить сферу информационной безопасности практически на все вопросы и отношения в информационной сфере, по сути, отождествляя информационную безопасность с информационной сферой.

Информационная безопасность общества, государства характеризуется степенью их защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности (экономики, науки, техносферы, сферы управления, военного дела, общественного сознания и т.д.) по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы страны информационным воздействиям на уровне как внедрения, так и извлечения информации. Уровень информационной безопасности определяется способностью нейтрализовать такие воздействия.

Субъектами информационной безопасности следует считать те органы и структуры, которые занимаются ее обеспечением. Это могут быть федеральные и региональные органы исполнительной, законодательной, судебной власти, органы местного самоуправления.

Технические средства обеспечения информационной безопасности - это средства, с помощью которых осуществляются меры по защите систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации.

Развитие и внедрение в различные сферы жизни общества новых информационных технологий, как и любых других научно-технических достижений, не только обеспечивает комфортность, но и нередко несет определенную опасность. Сегодня можно выделить следующие наиболее существенные группы информационно-технических опасностей, обусловленных достижениями научно-технического прогресса.

Анализ механизма политического воздействия защиты российского сегмента глобальной сети Интернет на обеспечение информационной безопасности Российской Федерации свидетельствует о том, что разработка и реализация его основных компонентов – важная задача общегосударственного масштаба, от решения которой зависит не только функционирование информационной организации, но и всей системы органов государственной власти.

Особое место в ней занимает создание эффективной и действенной системы управления процессом развития информационной организации, поскольку именно управление процессом формирования информационной структуры предопределяет его состояние и направленность, а также оказывает непосредственное воздействие на результативность обеспечения информационной безопасности государства. Это обусловлено тем, что система управления является наиболее уязвимым звеном процесса преобразований информационной организации. Недостатки такой системы невозможно компенсировать какими-то ни было значительными материальными, финансовыми или же другими ресурсами. Более того, десятилетний этап преобразований информационной сферы Российского государства только обострил проблемы, связанные с информационными ресурсами, формирующими основу потребностей информационной организации государства.

В целом же политическая и экономическая обстановка в России ставит перед руководством страны вопрос о необходимости поиска новых подходов к разработке, планированию и реализации направлений информационной организации. Задача состоит в том, чтобы исключить нерациональное и безответственное расходование государственных средств и вместе с тем обеспечить защиту информационного пространства страны. Не менее важно добиться политической поддержки по ключевым вопросам защиты информационного пространства со стороны всех ветвей и уровней власти, а также широкой общественности.

Таким образом, оптимизация политического механизма воздействия защиты информационного пространства на обеспечение информационной безопасности требует от органов власти всех уровней создание условий, при которых обеспечение информационной безопасности приобретет характер важнейшего приоритета общегосударственного уровня.

Оптимизация информационной организации являет собой объективную потребность преобразования информационной организации Российского государства, но при этом должны быть соблюдены условия, обеспечивающие ее перспективное развитие, и, прежде всего, вывод информационной организации России из состояния «выживания».

Деятельность же органов государственной власти страны по реализации полномочий в области информационной безопасности должна быть не только максимально эффективной, но и рациональной. При этом под «эффективностью» следует понимать степень реализации задач информационной безопасности. Рациональными же, по нашему мнению, являются такие действия, которые базируются на наиболее эффективном и перспективном решении.

Задачей субъектов управления различных уровней власти становится поиск наиболее рациональных способов (путей) обеспечения эффективного управления, независимо от всей совокупности существующих объективных и субъективных обстоятельств, сопровождающих принятие управленческих решений.

Главной целью совершенствования управления при этом выступает достижение наилучших результатов деятельности при наименьших затратах сил, средств и ресурсов, то есть – оптимизация системы. Важно заметить, что содержание этого процесса заключается не только в коррекции целей и средств деятельности в зависимости от ее результатов, но и в поиске наиболее рационального построения организационной структуры системы управления, научной разработке и внедрении новых моделей и технологий управления. При этом процесс оптимизации системы управления (механизма) должен охватывать не только отдельные структурные составляющие (элементы) системы, но и всю совокупность объектов и субъектов управления, взаимосвязей горизонтального и вертикального порядка, то есть иметь системный характер.

Оптимизация политического механизма в деятельности органов государственной власти по реализации задач защиты информационного пространства предполагает формулирование и реализацию научно обоснованных целей, принципов, задач деятельности организационной структуры. При этом важно заметить, что оптимизации (управленческим воздействиям с целью достижения наилучших результатов) должны подвергаться, в первую очередь, те сферы (уровни управления, структуры, элементы системы) деятельности, в которых допускается рассогласование в схеме «цель – средство – результат».

Оптимизация политического механизма по реализации задач защиты информационного пространства в Российской Федерации должна предполагать упорядочение и регламентацию деятельности органов государственной власти на основе результатов научных исследований в данной области, а самое важное – содержать научно-обоснованный алгоритм выработки оптимальных решений в интересах обеспечения информационной безопасности страны.

Мероприятия по оптимизации политического механизма воздействия защиты информационного пространства на информационную безопасность государства должны найти свое правовое закрепление в комплексной программе преобразования системы управления информационной организацией, направленной на достижение качественно новых результатов в области управления защиты информационного пространства в интересах гарантированного обеспечения информационной безопасности Российского государства.

Полномочия в области информационной безопасности и государственной системы защиты информации определяются Конституцией Российской Федерацией, федеральными законами «О безопасности», «Об информации, информатизации и защите информации», «О федеральных органах правительственной связи и информации» и иными нормативными и законодательными актами.

В настоящее время в Российской Федерации осуществляется попытка комплексного решения проблем управления информационной организацией. Тем не менее, обращает на себя внимание то, что в структуре органов государственного управления особое место занимает Совет Безопасности Российской Федерации, сосредоточивший функции государственного управления и ставший своего рода структурным подразделением Администрации Президента Российской Федерации по вопросам безопасности. Представляется, что это положение в настоящее время обусловлено экстремальностью условий реформирования в России. Хотя давно назрел вопрос о принятии федерального конституционного закона «О Совете Безопасности Российской Федерации», который бы более подробно установил его правовой статус, в том числе и функции по обеспечению информационной безопасности.

Принципиально важным для дальнейшего развития информационной организации государства является формирование единой ценностно-мировоззренческой среды, отражающей потребности и перспективы развития личности, общества и государства.

Главным условием и предпосылкой движения по пути оптимизации политического механизма является разработка единой общенациональной государственной идеологии.

В зависимости от векторности и общественной ценности принципиальных положений сформированной государственной идеологии и концептуальных основ политики Российского руководства находятся и дальнейшие этапы деятельности по созданию новой модели политического механизма защиты информационного пространства, обеспечения информационной безопасности и ее оптимизации в процессе развития внутри- и внешнеполитической обстановки.

Следующим важнейшим направлением оптимизации политического механизма воздействия защиты информационного пространства на обеспечение информационной безопасности является разработка и применение научной методологии деятельности субъектов политики в указанной сфере.

Речь в данном случае идет о выработке научно обоснованных направлений преобразования системы управления информационной сферой государства и осуществления на этой основе стратегического планирования развития его информационной организации.

Ранее отмечалось, что одной из наиболее значимых причин, определивших кризисное развитие информационной организации, является отсутствие осмысленной государственной политики в данной области. Это обстоятельство во многом определяется тем, что защита информационного пространства органами управления реализовывалось в отрыве от результатов исследований отечественной науки. И это при том, что в Российской Федерации по-прежнему функционируют десятки научно-исследовательских центров и структурных подразделений, занимающихся непосредственно этой проблематикой. В целом характерной чертой деятельности органов государственного управления всего последнего десятилетия стала невостребованность научного потенциала страны. Это свидетельствует о сознательном игнорировании научных основ решения важнейших задач в области защиты информационного пространства и обеспечения информационной безопасности государства.

Очевидно, что аналогичная потребность использования научного потенциала должна существовать и в России. При этом разработка научной методологии оптимизации деятельности органов государственной власти по реализации задач защиты информационного пространства не является самоцелью, а осуществляется в интересах обеспечения эффективности информационной безопасности страны и ее информационных ресурсов.

Мировой опыт свидетельствует, что рациональная стратегия обеспечения информационной безопасности должна основываться на долгосрочных планах, учитывающих характер внешних и внутренних информационных угроз, приоритетах по обеспечению информационной безопасности государства и реальных экономических возможностях.

Такие сложные и жизненно важные элементы структуры государства, как мультисервисная сеть передачи данных, государственная сеть связи, Интернет-порталы органов государственной власти, электронные архивы, библиотеки и хранилища данных и др., не могут нормально функционировать, ориентируясь лишь на текущие проблемы. Их развитие гораздо шире.

Поэтому защита информационного пространства в России должна исходить не только из текущих возможностей, но и из перспективных потребностей обеспечения информационной безопасности государства. Кроме того, эффективное функционирование информационной организации государства предполагает наличие четко отлаженной системы принятия и реализации согласованных решений, касающихся ее вопросов. В противном случае информационная политика может вырабатываться узким кругом лиц без должного прогнозирования и всестороннего обоснования, определяться только сложностями нынешней политической и экономической ситуации, что может обострить существующие проблемы и в перспективе привести к крупным политическим, экономическим и социальным просчетам.

Начиная с 2000 года, в этом направлении происходят подвижки, и в настоящее время планирование в области защиты информации и информационной безопасности обретает систематизированный и перспективный характер. Этому способствует позиция Президента Российской Федерации, указами которого была предусмотрена разработка программ и направлений развития информационного пространства страны, главными из которых являются: Основы государственной политики Российской Федерации по формированию информационного пространства России; Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов; Федеральная целевая программа «Электронная Россия» и др.

Вышеперечисленные документы были разработаны соответствующими федеральными органами исполнительной власти. Однако при этом не было предусмотрено финансирование указанных мероприятий из федерального бюджета. Это во многом снижает эффективность указанных выше документов.

Другим недостатком государственных планов и программ по формированию информационного пространства России является их ведомственный характер.

Причинами этого, на наш взгляд, во многом являются: отсутствие надлежащей системы разработки, обоснования, согласования, рассмотрения и утверждения таких программ и планов. До сих пор в процессе планирования развития компонентов информационной организации нет четкого представления о принципах, путях и подходах, которыми следует руководствоваться при формировании и практической реализации информационной политики России. Между тем накопленный опыт позволяет говорить о том, что на всех этапах подготовки и принятия решений по проблемам защиты информационного пространства необходимо:

* четкое формулирование целей, обоснование задач и определение временных этапов их решения при условиях приоритетного финансирования расходов на указанные цели;
* комплексное решение проблем, исключающее нерациональное использование средств, дублирование и параллеризм в решении задач одного порядка, которое обеспечивает экономию ресурсов:
* определение взаимоувязанной системы единых исходных параметров (качественных и количественных показателей) для всех планов и программ формирования и развития информационного пространства Российской Федерации;
* обеспечение системного взаимодействия разработчиков разноведомственных программ и планов, а также их корреляция с реальными экономическими и социально-политическими потребностями и возможностями государства;
* активное участие в решении проблем информационной безопасности всех ветвей власти, профессионалов, а также независимых экспертов, что потребует большей открытости и доступности информации, не наносящей ущерба безопасности страны.

Оптимизация политического механизма требует создания специальной системы (органа), координирующей деятельность субъектов информационной политики в масштабе государства.

В условиях действующей ныне Конституции России роль органа, в наибольшей степени предназначенного сочетать в своей деятельности координирующие и управленческие функции в отношении всех министерств и ведомств, а также органов государственной власти в части, касающейся реализации задач обеспечения информационной безопасности государства, может выполнить Совет Безопасности Российской Федерации, председателем которого является Президент России.

Координация деятельности органов управления представляет собой согласование, установление целесообразного соотношения между какими-нибудь действиями. Координация, в отличие от взаимодействия, не содержит в себе элемент подчинения воле координирующего органа. В отличие от этого взаимодействие организуется и поддерживается непосредственным подчинением управленческим инстанциям.

Координация деятельности органов государственной власти не является самоцелью, а ориентирована на достижение комплексного решения проблем защиты информационного пространства страны в интересах гарантированного выполнения поставленных задач.

Следует подчеркнуть, что при реформировании информационной организации, да и в целом решения задач в информационной сфере, важно руководствоваться исторически обоснованным принципом: дробление основных структур информационной организации государства, ослабление централизации управления ими не совместимы с ростом его защиты.

Именно поэтому для объединения усилий государственных органов, их региональных структур важно устранить возникающие между ними противоречия, разрушить устоявшиеся стереотипы, которые порождают «самостийность» и, в конечном счете, приводят к стихийным разобщенным действиям.

Заключение

Роль и значение информационной безопасности в обществе возрастают. Отставание в информатике может привести в перспективе к уязвимости компьютерных сетей страны и всей ее информационной, управленческой инфраструктуры.

Защита информационного пространства должна стать одной из значимых задач модернизации российской государственности, предопределяющей во многом содержание и динамику внутриполитических процессов в российском обществе, специфику самоидентификации Российского государства, определения его места и роли в трансформирующемся мировом сообществе.

Актуализация проблемы защиты информационного пространства и его влияния на информационную безопасность непосредственно связана с существующими реальными и потенциальными угрозами и вызовами безопасности государства, уровень и масштабы которых в последнее десятилетие многократно возросли и приобрели крайне опасный характер.

Информационный век приносит много новых вопросов, которыми должны заняться законодательная и исполнительные власти, - среди них онлайновая безопасность и удостоверение личности, конфиденциальность и защита данных, юрисдикция в киберпространстве и налогообложение электронной коммерции, правовые аспекты коммуникационного общения и ответственность за киберпреступления.

**Литература**

1. Закон РФ «Об информации, информатизации и защите информации» Принят Государственной Думой 25 января 1995 года (в ред. Федерального закона от 10.01.2003 N 15-ФЗ)

2. Закон РФ "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".)

3. Федеральная целевая программа "Электронная Россия» (2002-2010 годы)

4. Общая теория национальной безопасности: Учебник/Под общ. ред. А.А.Прохожева. - М.: Изд-во РАГС, 2002. -С.39.

5. Бочаров Е.П., Колдина А.И. Интегрированные корпоративные информационные системы: Учеб. пособие – М.:Финансы и кредит, 2005. Информационные технологии управления: Учеб. пособие для вузов / Под ред. Проф. Г.А. Титоренко – М.: ЮНИТИ-ДАНА, 2003.

7. Информационные технологии бухгалтерского учета :[Учебник для студ. и препод. эконом. спец. вузов и бухг.] /Ильина О.П. -СПб.: Питер, 2001.

8. Корнейчук Б.В. Информационная экономика. Учебное пособие. – СПб.:Питер, 2006.